IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

STEPHANIE SCHOLL and FRANK BEDNARZ, Plaintiffs, v. ILLINOIS STATE POLICE; BRENDAN F. KELLY, *in his official capacity as Director of the Illinois State Police*; JAY ROBERT PRITZKER, i*n his official capacity as Governor of the State of Illinois*; KWAME RAOUL, *in his official capacity as Attorney General of Illinois*, Defendants.	Case No. 1:24-cv-4435 Hon. Judge Martha M. Pacold **Plaintiffs' Response in Opposition to Defendants' Motion to Dismiss and Reply in Support of their Motion for Preliminary Injunction**

Introduction

Plaintiffs submit this brief in opposition to Defendants' Motion to Dismiss ("MTD"), see Dkt. 23, and in support of their own Motion for Preliminary Injunction ("PI Memo"), see Dkt. 15. Defendants' arguments misunderstand Plaintiffs' claim: Plaintiffs' injury in this case is not that the ALPR data might one day be used against them in a court of law, but that the collection of the ALPR data without constitutional process itself is an unreasonable search in violation of the Fourth Amendment. Defendants' misunderstanding dooms their arguments on both standing and the merits. Next, Defendants' arguments about immunity fall short: Plaintiffs seek injunctive relief, from which Defendants are not immune, against the officials responsible for overseeing and managing the implementation of the challenged polices. And Defendants have not raised immunity as to Defendant Kelly, so any claim for immunity as to him has been waived. Finally, Defendants' arguments against issuing a preliminary injunction fail because Plaintiffs have a likelihood of success on the merits and are harmed by the continuous collection of the ALPR

data, and the balance of harms favors the public's interest in the protection of their Fourth Amendment rights. This Court should therefore deny the motion to dismiss and grant Plaintiffs' motion for preliminary injunction.

Argument

I. Defendants are not entitled to immunity from Plaintiffs' claims for injunctive relief.

Defendants attempt to avoid scrutiny by invoking sovereign immunity, but this is not a suit for damages. "[A] federal court, consistent with the Eleventh Amendment, may enjoin state officials to conform their future conduct to the requirements of federal law." *Quern v. Jordan*, 440 U.S. 332, 337 (1979). And Defendants do not dispute that *Ex Parte Young*, 209 U.S. 123 (1908), permits federal courts to enjoin state officials to conform their conduct to requirements of federal law. *Milliken v. Bradley*, 433 U.S. 267, 289 (1977); *see* MTD 4–5. Injunctive relief against Defendant state officials Kelly, Pritzker, and Raoul is thus perfectly appropriate under 42 U.S.C. § 1983; sovereign immunity does not apply to these defendants. *MSA Realty Corp. v. Illinois*, 990 F.2d 288, 291 (7th Cir. 1993).

Defendants do not argue that Defendant Kelly is entitled to any sort of immunity or that he is not an appropriate official-capacity defendant. Sovereign immunity is waivable, and even if Defendant Kelly were entitled to it—which he is not—he has waived it. "Unless the State raises the matter, a court can ignore it." *Wis. Dep't of Corr. v. Schacht*, 524 U.S. 381, 389 (1998). Regardless of the merits of Defendants' claim of sovereign immunity for the agency which Kelly heads, the Illinois State Police, Plaintiffs' claims and request for injunctive relief as to Defendant Kelly are appropriate.

Defendants Pritzker and Raoul assert that sovereign immunity applies to them, and the Eleventh Amendment bars Plaintiffs claims against them, because neither Pritzker nor Raoul have specific involvement in enforcing the Act. In essence, Defendants' argument is that

injunctive relief against the Act's enforcement would apply only to Defendants Kelly and ISP, not to Pritzker and Raoul, because they supposedly have no official responsibilities under the Act. But Kelly and ISP work for the Governor and Attorney General, who have ultimate authority over their actions. Defendants Pritzker and Raoul each are proper parties under *Ex Parte Young* because they are the officials responsible for overseeing and managing the implementation of the challenged polices of the Act.

Defendants' own citation explains the distinction. In *Doe v. Holcomb*, 883 F.3d 971, 975 (7th Cir. 2018), the immigrant plaintiff challenged Indiana's name-change statute, which he was unable to take advantage of because it required proof of United States citizenship, and he was not a citizen. The Seventh Circuit pointed out that the plaintiff had not sued the governor in his capacity as head of the State Bureau of Motor Vehicles, whose policy based on the name-change statute was denying the plaintiff the ID with his preferred name: "Doe may have been able to overcome the Eleventh Amendment had he sued the Governor to enjoin the enforcement of the BMV's requirements. Instead, Doe sued the Governor in his official capacity to prevent him from enforcing the name-change statute." *Holcomb*, 883 F.3d at 976. This case is like the Seventh Circuit's hypothetical: Plaintiffs did not sue the Governor and Attorney General to prevent them from *enforcing* the Tamera Clayton Expressway Cameras Act. Rather, Plaintiffs' Complaint asks this court to enjoin the *implementation* of the Act and the ongoing *operation* of the ALPRs by ISP. Just as the Indiana Governor in *Holcomb* was the head of the Bureau of Motor Vehicles, here the Illinois Governor is the state official who has final authority over the policies and practices of ISP—he appoints the director, who reports to him—and the Attorney General of Illinois is the chief law enforcement officer of the state responsible for overseeing the criminal investigations and prosecutions derived from this unconstitutional surveillance. Both have a

direct role to play in and direct authority over the operation of the challenged program, and therefore are appropriate parties under *Ex Parte Young*. *See Entm't Software Ass'n v. Blagojevich*, 469 F.3d 641, 645 (7th Cir. 2006) (noting that "it is not necessary that the officer's enforcement duties be noted in the act")(quoting *In re Dairy Mart Convenience Stores Inc.*, 411 F.3d 367, 373 (2d Cir. 2005)). Eleventh Amendment sovereign immunity does not apply to Defendants Pritzker and Raoul, and the injunctive relief sought by Plaintiffs is appropriately applied against them.

II. Plaintiffs have standing to challenge the warrantless, suspicionless tracking of their movements.

The sole basis for Defendants' assertion that Plaintiffs lack standing is their insistence that "the Plaintiffs drive on roads that may have ALPRs, and that, alone, is their injury." MTD at 8. But that is not Plaintiffs' injury. Plaintiffs' injury is that "Defendants' warrantless, suspicionless, probable-cause-free tracking of their movements everywhere they drive in their car is a Fourth Amendment search that violates their connotational privacy interest in the whole of their physical movements." PI Memo at 3–4. The surveillance in this case is not incidental: it is systematic; it is not occasional: it is constant; it is not transient: the data is retained as a matter of policy; and it is not tied to the investigation or prosecution of any crime: rather it treats everyone as appropriate subjects for constant surveillance everywhere they travel.

Defendants argue that Plaintiffs' claims are "insufficient because Plaintiffs do not allege that ALPR data has ever been used against them in any way, [and] do [not] allege any reason to believe it will be," dismissing "Plaintiffs' undefined hypothetical injuries that may (or may not) happen sometime in the infinite future." MTD at 8–9. But Plaintiffs' injury is not hypothetical or in the future; it is currently occurring because their injury is in the ongoing tracking, regardless of what that data is used for in the future. The Fourth Amendment protects Plaintiffs from

unconstitutional searches—regardless of whether the government uses the fruits of a search against the person who was subjected to the search. Legal doctrines such as the exclusionary rule limit what police can do with improperly obtained information, but if the search itself was not a Fourth Amendment violation, the later use of the evidence would not turn it into one. Hence doctrines like inevitable discovery, *Nix v. Williams*, 467 U.S. 431 (1984), and the "good faith" exception, *United States v. Leon*, 468 U.S. 897 (1984)—exceptions to the exclusionary rule that the government may not rely on evidence obtained in violation of the Fourth Amendment. The question is therefore not whether "the State may misuse information about when [Plaintiffs] pass a particular portion of an expressway." MTD at 11. Rather, the question is whether the peremptory collection and retention of the data in the first place is unconstitutional.

No matter how many times Defendants repeat the assertion, it is simply not true that "Plaintiffs base their case on the hypothetical that one day, law enforcement could start culling through ALPR data to investigate them for vehicular hijacking, terrorism, motor vehicle theft, or another forcible felony, including one that involves the unlawful use of a firearm." MTD at 11, *see also* MTD at 10 ("Plaintiffs have done nothing more than raise the issue that, in their opinion, if they were to commit a specific subset of crime(s), law enforcement could use ALPRs-gathered data to link them to those crimes"). The surveillance itself is the search and violates the Fourth Amendment. If Illinois passed a law mandating a surveillance camera in every home's master bedroom, the injury would be the recording of the intimate details of our homes—a Plaintiff would not have to wait until police actually viewed the footage to challenge that search. The same is true here.

Defendants point out that Plaintiffs have not styled this case as a class action, MTD at 12–13, which is true, but for present purposes that is simply a question of the scope of the requested

preliminary injunction. An order from this Court that was limited to the specific plaintiffs in this case would still provide them needed protection from the violation of their rights, even if it would not completely protect them or prevent abuses of the system more broadly.

However, it is simply not the case this Court lacks the power to issue broader relief. As the Seventh Circuit has explained, "historical and current practice lends support to a determination that the courts possess the authority to impose injunctions that extend beyond the parties before the court." *City of Chicago v. Barr*, 961 F.3d 882, 916 (7th Cir. 2020). The governing law in this circuit is that "universal injunctions can be necessary to provide complete relief to plaintiffs, to protect similarly situated nonparties, and to avoid the chaos and confusion that comes from a patchwork of injunctions." *Id.* at 916–17 (internal quotation marks omitted). Indeed, "[a]ny number of factors could influence a court's determination as to the proper scope of an injunction, including the nature of the violation, the extent of the impact, the urgency of the situation, the multiplicity of litigation, and the ability of others to even access the courts." *Id.* at 917.

This case is precisely the sort of situation the Seventh Circuit contemplated in *Barr*. Although Plaintiffs would get some needed relief from a more limited preliminary injunction, complete relief would require this Court to issue a general injunction against the misuse of this data; it is not apparent that it would be possible for Defendants to stop tracking only the Plaintiffs with ALPRs. It will also protect similarly situated third parties, an interest recognized by the Seventh Circuit, *id.* at 916—the millions of other drivers in the Chicago area are in the same situation as Plaintiffs—and to the extent this Court finds that Plaintiffs are likely to succeed on the merits of their claims, that would also mean the other citizens of Cook County are inherently suffering the same irreparable harm. There is no reason, other than the strictest legal formalism, to require them to each bring thousands of individual lawsuits to assert the same

right. And "[t]he difficulties, expense and delay inherent in pursuing a class action would render it inadequate for th[is] type of situation." *Id.* at 917. It is therefore appropriate for this Court to enjoin Defendants' misuse of this mass surveillance system generally.

III. ISP's collection of ALPRs constitutes a search.

Defendants say it is unclear whether Plaintiffs have brought a facial or as-applied challenge, MTD at 13, but Plaintiffs bring this case as both: the program is facially invalid because its mass tracking of every citizen, whether innocent or guilty, is not a policy with any constitutional application; and of course it is also unconstitutional as applied to Plaintiffs specifically, whom Defendants have no reason to track or surveil indefinitely.

Defendants contend that Plaintiffs have given away the game on the facial challenge because their motion "references a potential constitutional use of ALPRs to locate a missing person." MTD at 14. But this again misunderstands Plaintiffs' claim, which is based on the *aggregation and retention* of ALPR data—the portion of Plaintiffs' memorandum to which Defendants cite is about real-time use to locate a car for which police have a specific reason to search. There are real privacy concerns, including constitutional concerns, with the misuse of real-time data like this—it doesn't seem that Defendants have sufficient guardrails preventing improper access, for one—but Plaintiffs recognize that the Fourth Amendment allows for greater latitude when there are exigent circumstances present, as there often will be when dealing with fleeing suspects or missing persons. *See generally Brigham City v. Stuart*, 547 U.S. 398 (2006); *Kentucky v. King*, 563 U.S. 452 (2011).

A facial challenge to real-time use *would* therefore face the problem that there are significant uses that are likely constitutional. Not so with the aggregation and storage of historical data: that is unconstitutional on its face because there is no probable cause, reasonable suspicion, or any other standard being applied at any point in the process, and no exception like exigent

circumstances or good faith that can apply. There's no emergency that necessitates tracking every citizen everywhere they go every day. Even as to those suspects eventually convicted of crimes, there was no reason to track them prior to the police investigating them, and therefore the tracking of them is likewise unconstitutional.

Defendants cite several cases for the traditional Fourth Amendment principle that things that take place in public are not afforded an expectation of privacy. MTD at 15 (citing *United States v. Knotts*, 460 U.S. 276 (1983); *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Jones*, 565 U.S. 400 (2012)). But *Knotts* is about an old-fashioned tail. 460 U.S. at 281. If *Knotts* controlled here, then *Jones*—which held that physical trespass onto a vehicle to place a GPS device constituted a search, 565 U.S. at 405–06—would have come out differently. The whole point of *Jones* is that *Knotts* does not answer these questions. *See Jones*, 565 U.S. at 409, 412–13; PI Memo at 4–5. And cases about an individual police officer's check of a vehicle registration in a database where the officer has a specific reason to check that registration also is not relevant. *See United States v. Miranda-Sotolongo*, 827 F.3d 663, 667–68 (7th Cir. 2016). ISP is not checking an individual's registration one at a time where there are specific circumstances; it is hoovering up every plate without any particular reason.

Defendants rely on *United States v. Tuggle*, 4 F.4th 505 (7th Cir. 2021), which held that "extensive pole camera surveillance in this case did not constitute a search . . . [because] the government's use of a technology in public use, while occupying a place it was lawfully entitled to be, to observe plainly visible happenings, did not run afoul of the Fourth Amendment." *Id*. at 511. But as Plaintiffs explained in their memorandum, the three cameras in *Tuggle* were recording in public at a single location: Tuggle's residence. PI Memo at 10. The cameras did not follow Tuggle around town, and they did not invade the interior of his home. There was therefore

no search because there was no expectation of privacy in what was taking place in public at a single location. In this case, by contrast, the data tracking follows Plaintiff across Cook County—and even beyond it, as the Vigilant system aggregates data nationally. *Tuggle* is not a case about the aggregation of physical movements across both time and space—it is simply about a single set of cameras at a single location.

Defendants' attempt to distinguish *Carpenter v. United States*, 585 U.S. 296 (2018) and *Leaders of the Beautiful Struggle v. Baltimore Police Dept.*, 2 F.4th 330, 342 (4th Cir. 2021), falls short. MTD at 16–18. Their main argument appears to be that "ALPRs (unlike the information discussed in *Carpenter* and *Leaders of the Beautiful Struggle*) do not even show the non-highway/expressway roads that an individual drives on, let alone the homes, businesses, doctor's offices, or any other actual locations." *Id.* Plaintiffs already addressed this argument in their memorandum in support of preliminary injunction, noting that "even relatively 'low resolution' data, when aggregated together, can tell the government a great deal about our lives." PI Memo at 7.

Here Plaintiffs will add a few points. First, Defendants' description is not accurate: the data available to ISP is not so limited: Defendants have access to data from any other jurisdiction that uses the Vigilant database and shares the data as ISP does. One of Defendants' own citations includes facts found by this Court that necessarily mean the FBI is using other Vigilant cameras in Cook County. *See United States v. Brown*, Case No. 19-cv-949, 2021 U.S. Dist. LEXIS 206153, at *3 (N.D. Ill. Oct. 26, 2021). Plaintiffs hope to clarify in discovery just what other data ISP has from what other jurisdictions—which might include many cameras in and around Cook County—but for now submit that the aggregate data of the ALPRs is enough to constitute an unconstitutional search. The Court in *Carpenter* could have looked at just the four specific data

points the government used against Mr. Carpenter at trial, but it recognized that this was not the proper analysis. Rather it looked at the *entirety* of the data the government collected. The entire point of *Carpenter* is that the aggregation of data is different. The data in *Leaders of the Beautiful Struggle* lacked much of the specificity of the data here—they couldn't actually run licenses plates against ownership records but just had a plane flying around recording the movements of car-shaped blobs. But as the Fourth Circuit explained that aggregation of blobs is enough, because if you put enough blobs together you get the equivalent data in *Carpenter*, since the constant recording of public movements provides all sorts of intimate details to those with no business knowing. 2 F.4th at 342.

Defendants also assert that "the ALPRs only gather data that is voluntarily displayed when the Plaintiffs drive on public roads from a location that the ISP is allowed to occupy." MTD at 18. Defendants appear to be invoking the third-party doctrine of *Smith v. Maryland*, 442 U.S. 735 (1979). *Smith* and the other third-party doctrine cases are irrelevant here. Plaintiffs have not provided data to a third party; the data is collected by *the government*. On this point, Defendants are on *weaker* grounds than the defendants in *Carpenter*, where the data *was* shared by the suspect with the third-party cell carriers. The data collection Plaintiffs challenge here is the *government's own* data collection. There is no third party that the government is getting the data from. Rather, *the government* is sharing the information with a third party—Vigilant—but that is not how the third-party doctrine works. Here, Plaintiffs have not voluntarily given information to a third-party; the government has taken that information against Plaintiffs' will.

Defendants cite *United States v. Brown*, Case No. 19-cr-949, 2021 U.S. Dist. LEXIS 206153, at *6 (N.D. Ill. Oct. 26, 2021), in which the Court denied a motion to suppress ALPR data. But Defendants ignore the rest of the opinion—the Court goes on to point out that cases like *Jones*

and *Carpenter* have replaced the analysis that Defendants rely on with a modern test concerned with aggregation. *Id.* at *8. The Court in that case simply found that the data in the record was insufficient to prove the *Carpenter* dragnet because the record only reflected a handful of datapoints. Defendants' reliance on *United States v. Porter*, Case No. 21-cr-87, 2022 U.S. Dist. LEXIS 6755 (N.D. Ill. Jan. 13, 2022), likewise entails much less data before the court, and is ultimately vitiated by the fact that the government in that case got a warrant for a physical GPS tracker in the end anyway—something Defendants are free do to at any point if they actually have reason to investigate someone.

Thus, Defendants' collection of ALPR data—warrantless, suspicionless, probable-cause-free tracking of Plaintiffs' movements everywhere they drive in their car—is a search that violates their Fourth Amendment rights.

IV. Plaintiffs' motion for preliminary injunction should be granted.

Defendants cite a variety of sources about irreparable harm, but their actual argument here is quite thin. *See* MTD 22–23. Defendants' argument is essentially about timing: that there is no irreparable harm because Plaintiffs waited too long to sue. *Id.* But Plaintiffs did not drag their feet in filing this case: like most citizens, they weren't immediately aware that this was happening—but they filed their complaint within months of becoming aware of the problem. The timing of Plaintiffs' suit did not prejudice Defendants in any way, and to hold otherwise would be to encourage gamesmanship. Plaintiffs timely filed this lawsuit and soon after filed for this preliminary relief. That they did not file an emergency motion to immediately enjoin the violation within 24 hours is something this Court should prefer: while this matter is vitally important, it is not that kind of emergency. Defendants' argument would require plaintiffs in general to file much more aggressive emergency motions more often, because anything less

would be evidence against their own argument. Plaintiffs submit this is not the approach this Court would prefer in the long run.

Defendants contend that Plaintiffs have an adequate remedy at law, but never quite identify one. MTD at 23. But even under *Ex Parte Young*, government officials are generally immune from damages claims, *see e.g.*, MTD at 4, which means there is no retrospective remedy available to Plaintiffs at the end of this case. By "adequate remedy at law," Defendants appear to mean that, were Plaintiffs ever prosecuted, they could file a suppression motion. MTD at 24. But that is not a remedy—Defendants again misunderstand Plaintiffs' injury. The injury to Plaintiffs is the ongoing tracking of their movements. They are suffering that injury already, and they have no other remedy for it—they cannot get damages from Defendants for the ongoing violation of their rights; and, in any event, damages would be inadequate to repair the injury suffered by Plaintiffs here. *See Orr v. Shicker*, 953 F.3d 490, 502 (2020) (defining irreparable harm as harm that cannot be repaired and for which money compensation is inadequate).

Defendants assert that the balance of harms favors the government because it has an interest in ensuring public safety. MTD at 25. But granting Plaintiffs' preliminary injunctive relief does appropriately balance the nature and quality of the intrusion on Plaintiffs' Fourth Amendment rights and the governmental interests at stake. *See Graham v. Connor*, 490 U.S. 386, 396 (1989). Plaintiffs seek a preliminary injunction that allows data to be collected but not accessed without a warrant supported by probable cause. This adequately protects the public safety interest—in any instance where law enforcement has a legitimate reason to search for the historical whereabouts of someone, it can get approval. If the government cannot meet that standard, the Fourth Amendment requires that the public's right to be secure in their persons against unreasonable searches must take precedence.

Thus, for the reasons stated here and in their motion, Plaintiffs have met the requirements for a preliminary injunction, and this Court should enter a preliminary injunction providing that Defendants may only access the collected data after obtaining a warrant.

Conclusion

For the foregoing reasons, Plaintiffs respectfully request that this Court deny Defendants' motion to dismiss and enter a preliminary injunction providing that Defendants may only access the collected data after obtaining a warrant.

Dated: October 10, 2024

Respectfully Submitted,

Stephanie Scholl and Frank Bednarz

By: /s/ Jeffrey M. Schwab
One of their Attorneys

Jeffrey M. Schwab
Reilly Stephens
Liberty Justice Center
7500 Rialto Blvd.
Suite 1-250
Austin, Texas 78735
512-481-4400
rstephens@ljc.org
jschwab@ljc.org